COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	rsync.net	ASV Company:	Comodo CA Limited
Date scan was completed:	03-13-2018	Scan expiration date:	06-11-2018

Part 2. Component Compliance Summary

Component (IP Address, domain, etc.):64.62.236.70	Pass ☑	Fail ☐

Part 3a. Vulnerabilities Noted for each Component

ASV may choose to omit vulnerabilities that do not impact compliance from this section, however, failing vulnerabilities that have been changed to "pass" via exceptions or after remediation / rescan must always be listed

Component	Vulnerabilities Noted per Component	Severity level	CVSS Score	Compliance Status		Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
				Pass	Fail	
64.62.236.70	FTP Supports Clear Text Authentication 21 / tcp / ftp	Low	2.6	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	SSH Protocol Versions Supported 22 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	SSH Protocol Versions Supported 2222 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	FTP Server Detection 21 / tcp / ftp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	SSH Server Type and Version Information 22 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	SSH Server Type and Version Information 2222 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	Service Detection 22 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	Service Detection 2222 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	Service Detection 21 / tcp / ftp	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	SSH Algorithms and Languages Supported 22 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	SSH Algorithms and Languages Supported 2222 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	Nessus SYN scanner 2222 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	Nessus SYN scanner 22 / tcp / ssh	Low	0.0	☑	☐	The vulnerability is not included in the NVD
64.62.236.70	Nessus SYN scanner 21 / tcp / ftp	Low	0.0	☑	☐	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.
Protect your target with an IP filter.

Part 3b. Special notes by IP Address

Component	Special Note	Item Noted	Scan customer`s description of action taken and declaration that software is either implemented securely or removed
64.62.236.70	Remote Access	Remote Access: 22 / tcp / ssh	
64.62.236.70	Remote Access	Remote Access: 2222 / tcp / ssh	

Part 3c. Special notes -- Full Text

Note

Load Balancing

As you were unable to validate that the configuration of the environment behind your load balancers is synchronized, it is your responsibility to ensure that the environment is scanned as part of the internal vulnerability scans required by the PCI DSS.

Directory Browsing

Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.

Remote Access

Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.

Pos Software detected

Due to increased risk to the cardholder data environment when a point-of-sale system is visible on the Internet, please 1) confirm that this system needs to be visible on the Internet, that the system is implemented securely, and that original default passwords have been changed to complex passwords, or 2) confirm that the system has been reconfigured and is no longer visible to the Internet. Please consult your ASV if you have questions about this Special Note.

Embedded links or code from out-of-scope domains

Note to scan customer: Due to increased risk to the cardholder data environment when embedded links redirect traffic to domains outside the merchant's CDE scope, 1) confirm that this code is obtained from a trusted source, that the embedded links redirect to a trusted source, and that the code is implemented securely, or 2) confirm that the code has been removed. Consult your ASV if you have questions about this Special Note.

Insecure Services / industry-deprecated protocols

Note to scan customer: Insecure services and industry-deprecated protocols can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, 1) justify the business need for this service and confirm additional controls are in place to secure use of the service, or 2) confirm that it is disabled. Consult your ASV if you have questions about this Special Note.

Unknown services

Note to scan customer: Unidentified services have been detected. Due to increased risk to the cardholder data environment, identify the service, then either 1) justify the business need for this service and confirm it is securely implemented, or 2) identify the service and confirm that it is disabled. Consult your ASV if you have questions about this Special Note.

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Addresses/ranges/subnets, domains, URLs, etc.

IP_ADDRESS:64.62.236.70

Part 4b. Scan Customer Designated “In-Scope” Components (Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.

64.62.236.70

Part 4c. Scan Customer Designated “Out-of-Scope” Components (Not Scanned)

Requires description for each IP Address/range/subnet, domain, URL